INTERNATIONAL PERSPECTIVES ON CRYPTOGRAPHY POLICY

Panel Chair
Dorothy E. Denning
Georgetown University, Computer Science Department
225 Reiss Science Building, Washington, DC 20057-1232

Panelists
Peter Ford
Attorney General's Department, West Block Offices
Queen Victoria Terrace, Parkes ACT 2600, DX 5678 Canberra, Australia

David Herson
Commission of the European Communities, Directorate-General XIII
Rue de la Loi 200, B-1049 Brussels, Belgium

Nigel Hickson
Department of Trade and Industry, Policy for IT Security
151 Buckingham Palace Road, London SW1W 9SS, U.K.

Panel Summary

Panelists from outside the United States will discuss their views on cryptography policy and national and international proposals and initiatives. Efforts within the Organization for Economic Cooperation Development (OECD) to write cryptography policy guidelines will be reviewed. The panelists will describe initiatives to establish a cryptography infrastructure within their countries and internationally to support the security needs of the global infobahn. They will discuss the role of trusted third parties or key escrow in encryption policy and infrastructure services, and issues that need to be resolved.

ARE CRYPTOSYSTEMS REALLY UNBREAKABLE?

Panel Chair
Dorothy E. Denning
Georgetown University, Computer Science Department
225 Reiss Science Building, Washington, DC 20057-1232

Panelists
Steven M. Bellovin
AT&T Research
600 Mountain Avenue., Murray Hill, NJ 07974

Paul Kocher
Independent Cryptography Consultant
P.O. Box 8243, Stanford, CA 94309

Arjen K. Lenstra
Citibank
4 Sylvan Way, Parsippany, NJ 07054

Eric Thompson
AccessData Corporation
560 South State Street, Suite J-1, Orem, UT 84058

Panel Summary

We often hear the claim that today's codes are unbreakable. But are they, their implementations, or the systems that use them really secure? This session will explore the strength of existing systems in terms of potential weaknesses in algorithms, protocols, implementation, and application environments. Speakers will explore mathematically secure designs vs. systems that are secure in practice and measures for quantifying security. Recent efforts in factoring, code breaking, and vulnerability analysis will be discussed, along with what developers and users can do to improve security.

THE MATHEMATICAL PRIMITIVES:
ARE THEY REALLY SECURE?

Arjen K. Lenstra
Citibank
4 Sylvan Way, Parsippany, NJ 07054

Panel Statement

Corporations are beginning to see that venturing out on the Internet with a homepage on the web is to increase visibility and to draw attention. Unfortunately the audience includes not only potential customers but also virtually all hackers worldwide. At least some of them will, intentionally or not, cause trouble.

Solutions to the resulting security problems are not hard to find on the net, since many software vendors now advertise “secure” versions of their products. This makes using the net really risky, because users might mistakenly believe they are well protected. The widely publicized and rather frequent news stories about network break-ins and imperfections in security software should dispel such illusions. It seems that our competence to secure the net cannot keep up with our desire to use it.

Despite the confusing array of security solutions, there are only a few mathematical primitives on which they are based. Even in faulty security products, the soundness of the underlying mathematics is hardly ever in question; it is the way it is used that causes the vulnerabilities. In this presentation I discuss the mathematical primitives, not the many slippery ways in which they are employed. I concentrate on the primitives themselves, the assumption of their soundness and will discuss the latest theoretical and practical developments.